Proceedings of the International Conference , "Computational Systems for Health & Sustainability"
17-18, April, 2015 - by R.V.College of Engineering,
Bangalore,Karnataka,PIN-560059

# Authentication Of Digital Image Based on DWT-SVD and TA

**Nagwar Pragnya**
M.Tech Student
Department of Computer Science & Engineering
Visvesvaraya Technological University
Belgaum, Karnataka, India

**Aravind Naik**
Assistant Professor
Department of Computer Science & Engineering
Visvesvaraya Technological University
Belgaum, Karnataka, India

Abstract—**Digital watermarking is a process in which data can be hide into other image or audio or document. This data can be anything like secret data or it may be data which provides authenticity. Data can be hide in spatial or in frequency domain. since frequency domain technique is more robust against different kind of signal and non-signal processing attacks. And watermark can be extracted by blind or non-blind techniques.in this paper we proposed blind image watermark techniques and watermark is embedded using frequency domain using discrete wavelet transform, singular value decomposition and torus automorphism technique. This method proves that it is robust against different signal and non-signal processing attacks and watermark can be extracted without cover image.**

Keywords—**Discretwavelettransform,dwt,singularvalue decomposition,svd,torusautomorphism,watermark.**

## INTRODUCTION

Watermarking is a field of information hiding which is used to hide proprietary information which we call watermark image or watermark data in digital media like photographs, digital music, or digital video. Sharing or distributing of digital images over the internet by the users became a common phenomenon. Hence Some times we need to prove ownership of the content which is uploaded to internet or sent from one place to another. Authenticity for such contents can be achieved by using watermarking technique. Where the owner information is added or embedded into the original cover image and sent or uploaded on internet the owner information is extracted from watermarked image as and when necessary.

Two steps are followed in watermarking, one is embedding method and other is extraction method. Embedding of information is done either by spatial domain or frequency domain. Spatial domain is very simple and old method used to embed the information which is not robust against signal and non-signal attacks. Attackers can easily obtain watermark image simply by changing brightness or contrast of image. Frequency domain embedding method where we find that it provides more robust against different kinds of attacks such as providing robustness against geometric attacks like rotation, cropping and scaling attacks. In frequency based embedding, host image is converted into frequency domain using some transforms, where watermark will be embedded into frequency coefficients and then inverse transform will be applied to get watermarked image.

In extraction stage, blind and non-blind. In blind method, watermark extraction requires both original and watermarked cover image. Where non blind method does not require original cover image of watermark, existing frequency based methods not only provides robustness against geometric attacks but also compatible to popular image processing standards[1]. Frequency images transforms include Discrete Wavelet Transform(DWT), Singular Value Decomposition (SVD) etc.

## RELATED WORK

Existing frequency based methods are more robust against geometric and other signal processing attacks and also compatible to popular image compression standards[1]. Possible frequency images transforms include Discrete Fourier Transform(DFT),Discrete Cosine Transform(DCT), Discrete Wavelet Transform(DWT) and etc.

One can find the characteristics of watermarking and watermarking applications in [1]. Bors and Pitas developed a method based on DCT transform[2], In which input image will be divided into blocks of size 8x8 and dct will be performed and from which few blocks are selected based on a gaussian network classifier decision and accordingly dct coefficients are modified in those blocks according to watermark. Cox[3] developed the his first DCT based watermarking algorithm in which he embedded watermark in dct domain that uses human visual system properties. In above methods either all the coefficients or few coefficients of the image are used in watermarking. The amount of embedded information is an important parameter because it influences the watermark transparency. If more the embedded information then lower the watermark transparency. In order to increase the transparency F Huang [4] proposed a hybrid dct and svd based watermarking, in which SVD transform and DCT are performed on the watermark and the original image, respectively. Only the singular values of the watermark are embedded into the DCT coefficients of original image. There also a few watermarking methods based on combination of DCT and DWT, one such technique was developed by [5, 6], in which they embedded the watermark in middle frequency coefficients dct of three level DWT of LL band of original image. This combination shows little improvement on DCT based methods. Some of researchers developed the watermarking techniques using combination of DWT and SVD, one such method was mentioned in[7], where SVD was applied to all the frequency bands in DWT domain and SVD was applied to the watermark as well, but it needs to store sub matrices of SVD of watermark while extracting the watermark from watermarked image. [8] developed a method similar to [8] but, these people embedded the singular values of watermark into yuv color space of host image. Bhagyashri[9] also used the DWT and SVD to watermark the host image, but she did little different than fore said methods, she embedded in high frequency image, which was constructed from HH band of DWT of input image and then SVD used to watermark. In this paper, we proposed a new blind watermarking method to watermark the input image using the combination of DWT, SVD and Torus automorphism. In which we watermarked the LL band of DWT of input image and SVD will be applied on block of size 8x8, where watermark is the binary image and which is scrambled using torus automorphism technique in order to alleviate the problem of burst errors and this method gives good results against different kind of signal processing attacks. In section III we see the basics about wavelet transform, singular value decomposition and torus automorphism. Section IV gives process of embedding and extraction. Section V shows practical results of the algorithm and finally in Section VI concludes the paper.

## DISCRETE WAVELET TRANSFORM,SINGULAR VALUE DECOMPOSITION AND TORUS AUTOMORPHISM

### *A. Discrete wavelet transform*

Wavelet gives the time-frequency representation of the given signal. Wavelets are a set of non-linear bases. These bases are selected based on the function being approximated. Wavelets employ the dynamic set of bases functions in order to represent the given signal in most efficient way unlike static bases families [9]. DWT is very much suitable to identify the frequency regions of the image signal where watermark can be embedded effectively. The figures 1 and 2 depicts the simple structure of forward wavelet transform and inverse wavelet transform using filter banks.

### *B. Singular value decomposition (SVD)*

Singular value decomposition is a numerical technique which decomposes the input data into three sub matrices.

$$I=U*S*V^T$$

Where I is input signal, Uis left singular vector matrix,V is right singular vector matrix, and S is the diagonal matrix whose diagonal elements are singular values of given signal and these are also called as eigenvalues of the given signal. These singular values represents the energy of the signal. Because of translation, scaling properties of SVD it can be used as a tool to develop watermarking schemes[10].


***Fig 1. Example of 2D wavelet transform on image***

### *C. Torus automorphism*

In this method, we insert each watermark bit into SVD of one block of LL band of host image, before inserting the watermark, the binary watermark is spatially dispersed using a chaotic system called torus automorphism. Due this we can avoid burst errors. Torus automorphism is a kind of dynamic system. Briefly speaking, a dynamic system is a system whose states change with time t. When t is discrete, a dynamic system can be presented as an iteration of a function f, i.e., St+1 = f(St),t Z = 0, 1, 2, . . ., St , St+1 are the states at time t and t+1, respectively. A two-dimensional Torus automorphism can be considered as a permutation function or a spatial transformation of a plane region. This transformation can be performed using a 2x2 matrix A with constant elements[13]. The automorphism produces same image after few iterations. We are getting same image after 12 iterations. So this automorphism is periodic in nature. The figure 2 shows the example of torus automorphism on watermark and watermark images shown from left to right from t=0 to t=5.


***Fig 2. Example of torus automorphism from t=0 to t=5***

## WATERMARK EMBEDDING AND EXTRACTION

This section provides details about watermark embedding and watermark extraction process

### *D. Watermark Embedding*

Watermark is the customer related information in the form of binary data. Binary data can be either logo or bits representing customer ID. In this work we considered logo as a customer information. First, 2D logo will be converted into bits consists of zeros and ones and then resultant will be scrambled using torus automorphism upto five times, so that resultant data will be sparse in plane and this causes in reduction of burst errors and provides watermark security. The resultant data will be converted into bipolar form and re arranged as a 1D signal. This data acts as watermark that is going to be embed in the image. On the other hand one level 2D DWT will be applied on input image, in which watermark to be embedded. Then we select LL band as a host data, to embed watermark to it. LL band will be subdivided into blocks of size 8x8 and then SVD will be applied to each of the blocks. This results in a three matrices U*S*V’. We embed one watermark bit to one individual block that too to largest eigen value and then inverse SVD will be performed. Uniqueness of our technique is that, we embed one watermark bit to one individual block in SVD domain. So that this bit distributes over 64 pixels, even though we loss some data, we will be able to extract that bit. The embedded equations 2 to 4 is given below.

$$[U\ S\ V]=SVD(I_{block})$$

$$Watermark(i1,j1)=((S1(2,2)-S(3,3)*alpha1)/alpha2)$$

where _1 and _2 are scaling factors. And alpha1 and alpha2 are constant factor. Increase in scaling factor results in a decrease in PSNR and the watermark extraction is robust. So, we need to a compromised scaling factor. The said process is depicted in figure 3.

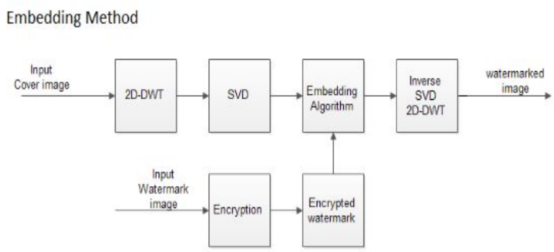


***Fig 3 Watermark embedding process***

### *E. Watermark Extaction*

Where, watermark extraction method is a blind that means it does not require original cover image while extracting watermark. So, if we have watermarked image that is enough to extract watermark. First, one level 2D DWT is computed on watermarked image and LL band of watermarked image will be divided into sub-blocks of size 8x8 and then block wise svd will be performed. We extracts watermark just opposite of embedding equation. Resultant image is re-arranged as matrix and then torus automorphism will be performed to get original logo. Watermark extraction procedure is as shown in fig 4.

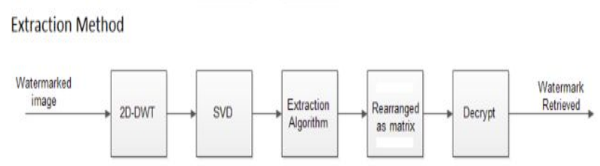


***Fig 4 watermark extraction process***

## RESULTS

This section describes some of the simulation results. We have selected the input image of size 512x512 and watermark logo of size is 32x32 and_1 and _2 are 1.5 and 7 respectively. We also see how the alpha changes results for different attacks. The following table gives the results interms of bir error rate(BER) against different attacks. These results are produced using MATLAB. From the results we can say that this method

TABLE I. BER TABLE

| S.No | Attack Type | BER $\alpha1$ =1.5 and $\alpha2$ =7 |
|---|---|---|
| 1 | - | 0 |
| 2 | JPEG compression(lossy) | 0.29 |
| 3 | Resize(120%) | 0.45 |
| 4 | Resize(50%) | 4.7 |
| 5 | Gaussian filtering | 9.03 |

is more robust against compression and resize attacks and filtering attacks, and not very robust against rotation attack for a given _1 and _2. As the watermark is added in blocks of 8x8 size performance against rotation attacks is weak. But we can still reduce errors by adding the watermark in center part of the LL band and in all sub-bands repeatedly and we can also use error correcting codes to reduce error. It is observed that in the case of rotation attack, burst errors are occurred at boundaries of the image

## CONCLUSION

In this work, we proposed a block based blind image watermarking using DWT,SVD and Torus automorphism and also proved that this method is robust against different kinds of geometric and non-geometric, signal and non-signal processing attacks. Further we can make this method more robust against different filtering attacks by applying same embedding method as we followed in this paper to all sub bands of the host image in DWT domain. This can be made robust against rotation either by increasing block size or adding the watermark at center region of the host image sub-band in DWT domain.

## REFERENCES

[1]. Vidyasagar M. Potdar, Song Han, Elizabeth Chang A Survey of Digital Watermarking Technologies. 3rd International Conference on Industrial Informatics 2005.

[2]. Bors and I. Pitas, Image wate rmarking using DCT domain constraints. in Proc. IEEE. Int. Conf. Image Processing , Lausanne, Switzerland, Sept. 1996, pp. 231-234.

[3]. Cox, IJ, Miller, ML Bloom, JA 2002, Digital Watermarking,Morgan Kaufmann Publisher, San Francisco, CA, USA..

[4]. Fangjun Huang, Zhi-Hong Guan, A hybrid SVD-DCT watermarking method based on LPSNR, Pattern Recognition Letters 25 (2004) 17691775..

[5]. W.H. Bin, Y.H. Liang, W. C. Dong, W.S. Ming: A New Watermarking Algorithm Based on DCT and DWT Fusion,” International Conference on Electrical and Control Engineering, pp. 2614 - 2617, 2010.

[6]. A. Al-Haj: Combined DWT-DCT digital image watermarking, Journal of Computer Science 3 (9): pp. 740- 746, 2007..

[7]. Emir Ganic , Ahmet M. Eskicioglu,Robust DWT-SVD domain image watermarking: embedding data in all frequencies, ACM Multimedia and Security Workshop 2004.

[8]. V.Santhi and Dr. Arunkumar Thangavelu, DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space, International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October2009 1793-8201.

[9]. Ms.Kapre Bhagyashri S, Mrs. Joshi M.Y, Robust Image Watermarking based on Singular Value Decomposition and Discrete Wavelet Transform, 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010, Pages 337 341.

[10]. Musawir Ali, An introduction to wavelets and haar transform, Available:http://www.cs.ucf.edu/ mali/haar/

[11]. Krishna Rao K, Srinivasa Rao Ch, ”Digital Audio Watermarking Using DWT-SVD and Secret Sharing,” International Journal of Signal Systems, Vol. 1, No. 1, pp. 59-62, June 2013

[12]. P. L. Lin, C.K. Hsieh and P.W. Hua ng, A hierarchical digital watermarking method for image tamper detection and recovery, Pattern Recognition,vol.38,no.4,pp.2519-2529,2005

ISSN 2320 –5547
IJITR International Journal of Innovative Technology and Research